Matthew J. Preusch (298144)
KELLER ROHRBACK L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
(805) 456-1496, Fax (805) 456-1497
mpreusch@kellerrohrback.com

Lynn Lincoln Sarko, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900, Fax (206) 623-3384
lsarko@kellerrohrback.com

Attorneys for Plaintiffs
Additional Attorneys Listed on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

KERRI MURPHY, ASHLEY CASHON, JADE HAILESELASSIE, ROY BISHOP, BRUCE MATTOCK, REESA ALI, TOM W. HANNON, and NANCY GAUGER et al., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

No.

CLASS ACTION COMPLAINT

JURY DEMANDED

Judge:

Table of Contents

Plaintiffs bring this action on behalf of themselves and all others similarly situated, against Equifax, Inc. ("Defendant"). Plaintiffs allege the following based upon information and belief, the investigation of counsel, and personal knowledge as to the factual allegations pertaining to himself/herself.

I. INTRODUCTION

1. Equifax, one of the nation's three large credit reporting agencies, trades in the personal information of tens of millions of Americans. Those who trust that information to Equifax have a right to expect that it uses the best possible information security infrastructure and practices. Unfortunately for nearly half of the nation's population, that appears not to have been the case.

2. On September 7th, Equifax disclosed that it had experienced a data breach that has exposed the most sensitive identifying information of 143 million Americans (the "Data Breach"). That includes names, dates of birth, and Social Security numbers: the essential raw materials for identity thieves. The breach also exposed phone numbers, credit card numbers, and driver's license numbers.

3. The Data Breach appears to have occurred in May, and does not appear to have been technically sophisticated. Rather, hackers were able gain access through a common web application with a known vulnerability that reportedly was not properly secured.

4. Once the hackers had access, they had more than two months to search for and obtain the most valuable information for identity thieves before Equifax discovered the breach. Although Equifax knew about the breach by July 29, it did not tell the tens of millions of victims of that breach until September 7th. And Equifax's response since then has been, to put it charitably, bumbling.

5. As a result of Equifax's negligence, tens of millions of Americans are now at increased risk of financial account fraud, tax fraud, and other forms identity theft. That increased risk will last for years, because the non-changeable identifying information has absolutely no shelf life.

6. To redress that and other harms caused by what is already being called the worst consumer data breach in history, Plaintiffs brings this action on behalf of themselves and a proposed nationwide class of similarly situated victims, seeking all available remedies.

II. PARTIES

A. Plaintiffs

1. Class representative Kerri Murphy is a U.S. Citizen and a resident of San Francisco County in the State of California. Ms. Murphy's data was compromised damaged and otherwise put at risk by Equifax's gross negligence and other violations of law.

2. Class representatives Ashley Cashon and Jade Haileselassie are U.S. citizens and residents of the Charleston County in the State of South Carolina. Both representatives' personal confidential data was compromised by Equifax's gross negligence and other violations of law

3. Class representative Roy Bishop is a U.S. citizen and a resident of Monroe County in the State of Florida. Roy Bishop's confidential personal financial data has been stolen, hacked or otherwise compromised through Equifax's gross negligence and other violations of law

4. Class representative Bruce Mattock is a U.S. citizen and a resident of Allegheny County in the State of Pennsylvania. Bruce Mattocks' data was compromised damaged and otherwise put at risk by Equifax's gross negligence and other violations of law.

5. Class representative Reesa Ali is a U.S. Citizen and a resident of San Mateo County in the State of California. Ms. Ali's data was compromised damaged and otherwise put at risk by Equifax's gross negligence and other violations of law

6. Class representative Tom W. Hannon is a U.S. Citizen and a resident of Maricopa County in the State of Arizona. Mr. Hannon's data was compromised damaged and otherwise put at risk by Equifax's gross negligence and other violations of law.

7. Class representative Nancy Gauger is a U.S. Citizen and a resident of Hartford County, Connecticut. Ms. Gauger's data was compromised damaged and otherwise put at risk by Equifax's gross negligence and other violations of law.

B. Defendant

8. Equifax Inc. is a global company headquartered in Atlanta, Georgia that does business throughout the country, including California, has offices throughout the State including in San Rafael, Concord, and Palo Alto, and is one of the three primary credit reporting agencies in the United States. Equifax maintains data on more than 820 million consumers worldwide. The company employs

approximately 9,900 people and operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. Among Equifax's subsidiaries is Equifax Information Services, LLC, which collects and report consumer information to financial institutions

III. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 based on the federal statutory claims below, and the Court has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367.

10. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one defendant, there are 100 or more Class members nationwide, and the aggregate amount in controversy exceeds $5,000,000.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(3) because the Court has personal jurisdiction over Defendant, a substantial portion of the alleged wrongdoing occurred in this District and California, and Defendant has sufficient contacts with this District and California.

12. Venue is proper in the Northern District of California pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims at issue in this Complaint, with over 15 million Californians impacted, arose in this District.

IV. INTRADISTRICT ASSIGNMENT

13. This action is properly assigned to the San Francisco or Oakland Division of this District pursuant to N.D. Cal. L.R. 3-2, because a substantial part of the events or omissions giving rise to Plaintiffs' claims arose in the counties served by the San Francisco and Oakland Divisions. Several of the named Plaintiffs and proposed Nationwide Class representative(s), as well as thousands of other Class members, who have had their personally identifying information breached, reside in the counties served by this Division.

V. FACTUAL ALLEGATIONS

A. Equifax Was Negligent in Its Efforts to Protect Highly Valuable Personal Information

14. Equifax is one of the largest credit reporting agencies in the world. It profits by reporting on people's most sensitive financial information. Hackers were able to gain access to that information

not as a result of a complex attack; rather, they exploited a known flaw in a common open-source web development software.

15. The hackers, according to the company, "exploited a U.S. website application vulnerability to gain access to certain files." This vulnerability is a part of a software package for building web applications called Apache Struts. Two vulnerabilities of that software package have been reported in 2017. In other words, the vulnerability was well known.

16. Equifax has represented that it has adequate data security measures that comply with applicable consumer protection laws. For example, in a 2011 report, "Leading With Integrity: The Equifax Business Ethics and Compliance Program," Equifax explained that the Gramm-Leach-Bliley Act required financial institutions to "develop and maintain an information security program to protect the security, confidentiality and integrity of the information." The report also represented that "Equifax entities that receive and collect consumer and customer information have developed and maintain appropriate information security programs."

17. Nonetheless, it appears Equifax did not have sufficient infrastructure or procedures to prevent the intrusion. It also appears that Equifax did not have sufficient infrastructure or procedures to detect the intrusion once it occurred. Once the hackers were able to gain access, they appear to have had that access for over *two months*, which suggests Equifax had very poor security detection practices.

B. Equifax Failed to Release News of the Massive Breach Within a Timely Manner, and Its Response Has Been Deeply Flawed

18. Equifax reportedly discovered the Data Breach in July, but did not disclose the breach to the American public until September 7th. For weeks, consumers were unaware that some of their most valuable private information could be open seen and used by anybody. This personal information could include data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history, which all factor into credit scores.

19. The impact of Equifax's delayed disclosure has been compounded by a botched response rollout, causing affected individuals additional harm and frustration. As computer security expert Brian Krebs wrote, "I cannot recall a previous data breach in which the breached company's public outreach

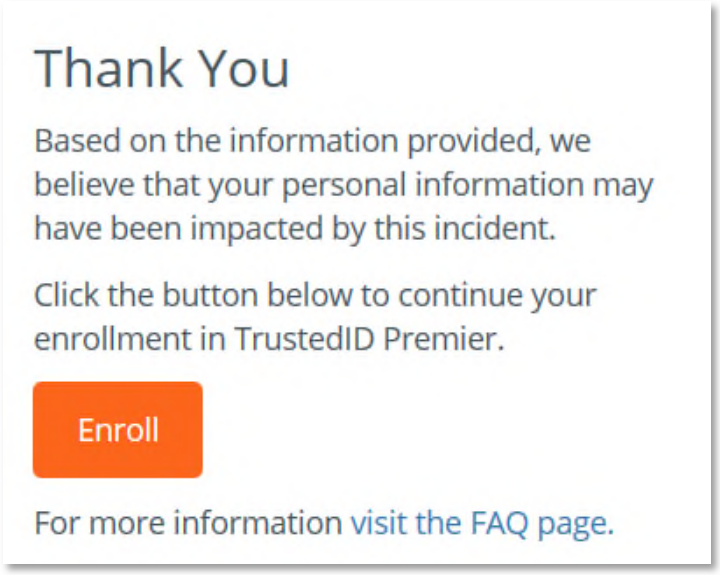
and response has been so haphazard and ill-conceived as the one coming right now from big-three credit bureau Equifax."

20. To begin with, the website that Equifax created to belatedly notify people of the Data Breach, www.equifaxsecurity2017.com, wrote Krebs, is "completely broken at best, and little more than a stalling tactic or sham at worst." For example, the website operates on a stock installation WordPress, which does not provide adequate security for website on which Equifax asks data breach victims to provide their last names and most of the Social Security number number. As another indication of Equifax's slipshod approach, as reported by Ars Technica, Equifax left a username for administering the site in a page hosted on that site, "something that should never have happened":

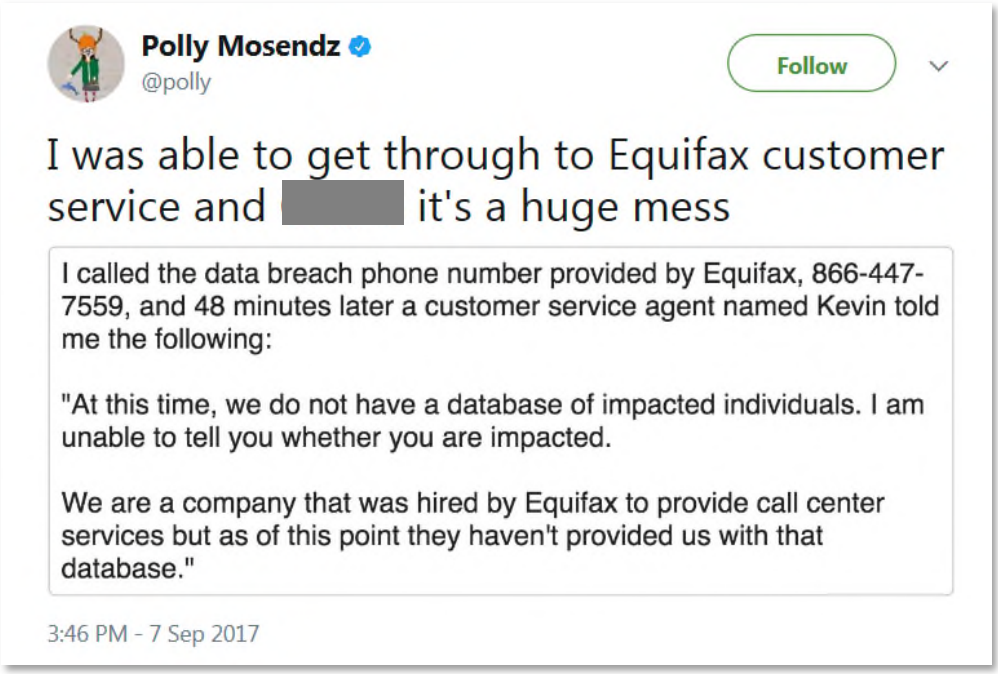
21. Those victims who were able to access the Equifax website to verify if they were victims of the Data Breach encountered more evidence of Equifax's bumbling response. To use the website, it appeared that Equifax was asking victims to give up any right to sue TrustedID, an Equifax entity providing identity monitoring services. Equifax appears to have changed the terms of service for that website after an outcry from consumers and consumer protection officials.

22. Aside from potentially luring victims into jeopardizing their right to sue, the Equifax website did not provide victims useful information on which they could act to protect their identities. Some victims who checked the website and were told they had not been affected were given the opposite answer when they checked later on a phone using the same information.

23. For example, entering two made-up identities—last names "Smith" and "Doe," both with the last six Social Security number digits "123456"—yielded the same response:



24. Those victims who called the hotline set up to aid Equifax victims fared little better. They were greeted by unprepared customer service agents without any helpful information. This complaint provides one example:



25. If a victim set up a credit freeze, Equifax provided a 10-digit personal identification number ("PIN"). Such PINs are supposed to be difficult to guess, but the PINs Equifax is providing are based on the time and date the person set up a freeze; thus, undercutting one of the key tools victims can use to prevent identify theft.

C. Equifax's Failures Have Harmed and Will Continue to Harm Breach Victims

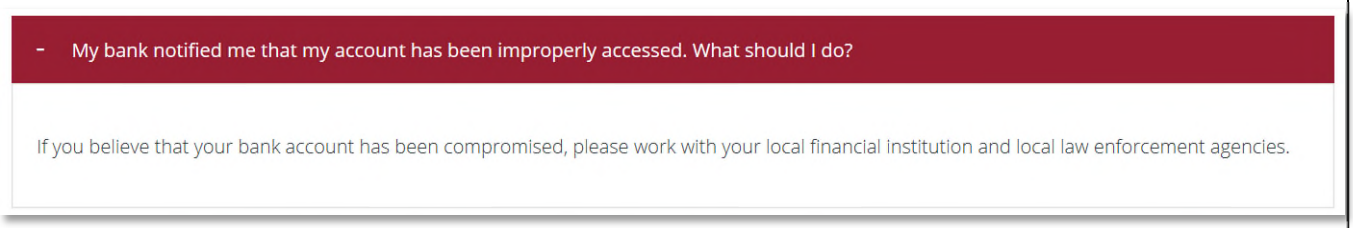
26. While Equifax's response to the Data Breach has been almost comically inept, the harm for victims is terribly serious. As a result of the Data Breach, criminals now have access to the essential building blocks to steal the identities of 143 million Americans, roughly 44 percent of the population.

27. The Equifax Data Breach has greatly increased the victims' risk of identity theft relative to the time before the Data Breach. Unlike the credit and debit card numbers stolen in some of the other recent high-profile data breaches, much of the information furnished here cannot simply be changed, and will continue to be valuable to identity thieves for many years.

28. As the Government Accountability Office reported in 2012, individuals who experience a data breach involving their Social Security number and dates of birth experience a much higher likelihood of being a victim of an identity crime. Social Security numbers, dates of birth, and names "are among the three personal identifiers most often sought by identity thieves," according to the GAO.

29. The Equifax Data Breach released all those personal identifiers, putting victims at risk of credit/debit card fraud, financial identity theft, tax fraud/identity theft, account takeovers, social identity fraud, and other harms.

30. Equifax's website for providing information to Data Breach victims acknowledges that they may already have experienced identity theft, including an answer for people who have been notified by their bank that their account "has been improperly accessed":



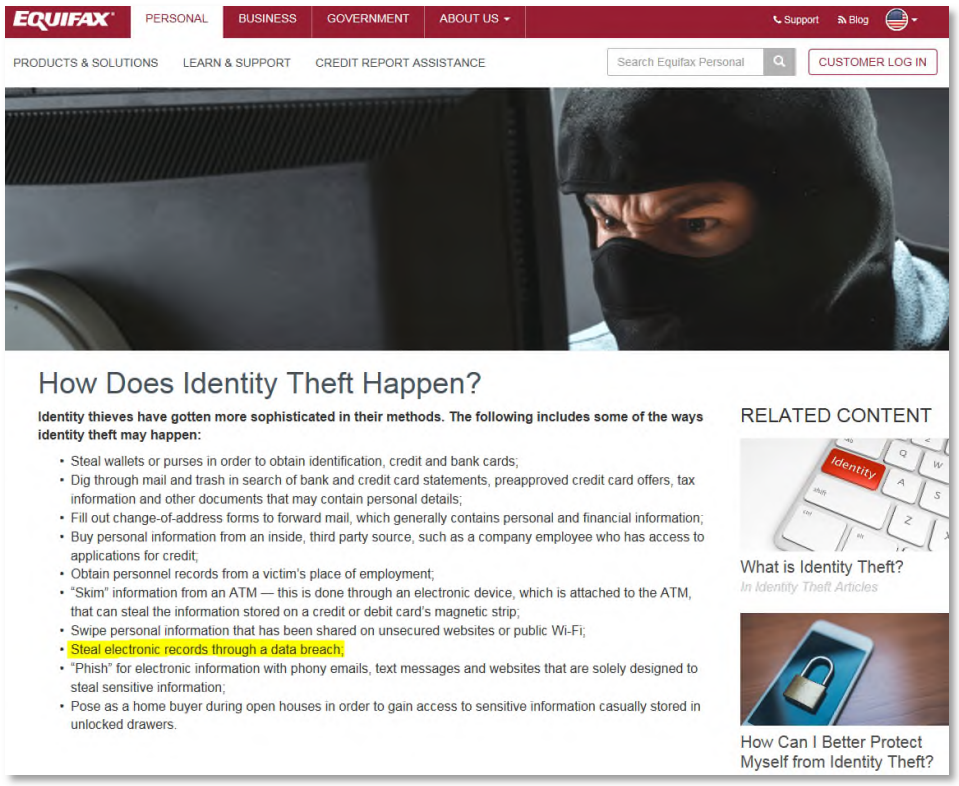
31. The same website recommends that victims "remain vigilant for incidents of fraud and identity theft[.]"

32. Equifax was aware of the increased risk of identity theft that data breaches cause, and the impacts of that identity theft.

33. Equifax has published a pamphlet called "A Lasting Impact: The Emotional Toll of Identity Theft" discussing the "real" impacts that identity theft victims face, which advises that to avoid identify theft people should keep their Social Security numbers, drivers licenses, and addresses private.

34. Elsewhere, Equifax explained that to protect themselves from identify theft, people should "[k]eep your personal information secure online" and "[s]ecure your Social Security Number."

35. One way identify theft could happen, Equifax warned, was the theft "of electronic records through a data breach":



36. Equifax has also acknowledged the increased risk that victims face by offering victims a one-year trial period of its proprietary credit monitoring service, TrustedID. But victims' increased risk of identity theft will last far beyond that one-year period. Identity thieves commonly wait years to commit fraud using breached data.

37. While victims are left vulnerable to identify theft, three top Equifax executives may have cashed out on the Data Breach, reportedly selling millions of dollars of stock after the company became aware of the breach but before the public found out.

VI. CLASS ACTION ALLEGATIONS

A. Class Definition(s)

1. National Class

38. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek relief on behalf of themselves and as representatives of a proposed nationwide class ("Nationwide Class"), defined as

follows:

> All natural persons in the United States whose personally identifying information ("PII") was compromised as a result of the Data Breach.

2. Statewide Classes

39. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert claims under the laws of individual states, and on behalf of separate statewide subclasses, for each of the following states:

a. Arizona

b. California

c. Connecticut

d. Florida

e. Pennsylvania

f. South Carolina

Each proposed statewide class ("Statewide Class") is defined as follows:

> All natural persons who are citizens of [STATE] whose PII was compromised as a result of the Data Breach.

40. Except where otherwise noted, "Class" or "Class members" shall refer to members of the Nationwide Class and each of the Statewide Classes.

41. Excluded from the Class are Defendant and any of its affiliates, parents or subsidiaries; all employees of Defendant; as well as the Court and its personnel presiding over this action.

42. **Numerosity.** The proposed Class is sufficiently numerous, as 143 million Data Breach victims had their PII compromised, and they are dispersed throughout the United States, making joinder of all members impracticable. Class members can be readily identified and ascertained through the records maintained by Equifax.

43. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members, including:

a. Whether Equifax had a legal duty to use reasonable security measures to protect Class members' PII;

b. Whether Equifax timely, accurately, and adequately informed Class members that

their PII had been compromised;

c. Whether Equifax breached its legal duty by failing to protect Class members' PII;

d. Whether Equifax acted reasonably in securing Class members' PII;

e. Whether Class members are entitled to actual damages and/or statutory damages; and

f. Whether Class members are entitled to injunctive relief.

44. **Typicality.** Plaintiffs' claims are typical of the claims of members of the proposed Class because, among other things, Plaintiffs and Class members sustained similar injuries as a result of Equifax's uniform wrongful conduct and their legal claims all arise from the same conduct by Equifax.

45. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Plaintiffs' interests do not conflict with other Class members' interests and they have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class.

46. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Equifax's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

47. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Equifax has acted or refused to act on grounds that apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

48. Rule 23(c)(4). This action also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims of Class members are composed of particular issues that are common

to all Class members and capable of class wide resolution that will significantly advance the litigation.

VII. CLAIMS FOR RELIEF

Claims Asserted on Behalf of the Nationwide Class:

COUNT I — WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. § 1681, *ET SEQ.*

1. Overview

49. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

50. Plaintiffs and the Class bring this claim to recover damages suffered as a result of Equifax's below-described willful violations of the Fair Credit Reporting Act (herein, "FCRA" or "the Act"), 15 U.S.C. § 1681 et seq.

51. As individuals, Plaintiffs and Nationwide Class members are consumers entitled to the protections of FCRA. 15 U.S.C. § 1681a(c).

52. Congress, in enacting FCRA, found that "[c]onsumer reporting agencies," like Equifax, "have assumed a vital role in assembling and evaluating consumer credit and other information on consumers" and, as a result, "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, *and a respect for the consumer's right to privacy*." 15 U.S.C. § 1681(a)(3)-(4) (emphasis added).

53. Under FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

54. Equifax is a consumer reporting agency under FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

55. Congress further noted that one purpose of the Act is to "require that consumer reporting agencies *adopt reasonable procedures* for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, *with regard to the confidentiality*, accuracy, relevancy, *and proper utilization of such information*." *See*

15 U.S.C. § 1681(b) (emphasis added).

56. As detailed below, Equifax failed to fulfill its statutory obligations under the Act by, at a minimum: (a) failing to adopt reasonable procedures to protect the confidentiality, privacy, and proper utilization of Plaintiffs' and the Nationwide Class members' personal consumer, credit, and other personally-identifying information including names, social security numbers, credit card numbers, account numbers, credit histories and other credit data; (b) furnishing and/or disclosing that information to improper third parties; (c) failing to take swift action upon learning of unauthorized access to Plaintiffs' and the Nationwide Class members' personal information and its unauthorized dissemination to third parties; and (d) disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and Nationwide Class members.

2. Violations of 15 U.S.C. §1681e(a) – Willful Failure to Maintain Reasonable Security Measures

57. 15 U.S.C. § 1681e(a) requires that "consumer reporting agenc[ies]," such as Equifax, "shall maintain reasonable procedures designed to avoid violations of section 1681c of this title and to limit the furnishing of consumer reports to the purposes listed under [15 U.S.C. § 1681b]." 15 U.S.C. § 1681e(a).

58. These procedures, the Act goes on to explain: "shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose." *Id*.

59. Moreover, the Act directs that "[n]o consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a [permissible] purposed listed in section 1681b of this title." *Id*.

60. The Federal Trade Commission has explained that 15 U.S.C.§ 1681e(a) requires consumer reporting agencies to "have reasonable and effective procedures to limit unauthorized access to its databases. Such procedures may include a system of monitoring access to its database of consumer reports, including a system to monitor anomalies and other suspicious activity to guard against unauthorized access . . . . Procedures also may include . . . installation and use of appropriate computer hardware and software. . . ." Fed. Trade Comm'n, *40 Years of Experience with the Fair Credit Reporting Act* at 66 (July 2011).

61. And, the Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

62. Equifax violated Section 1681e(a) by failing to implement and maintain reasonable, industry-standard security measures to ensure that Plaintiffs' and the Nationwide Class members' consumer credit information was not accessed for an impermissible purpose.

63. Equifax further violated Section 1681e(a) by failing to require prospective users of information to identify themselves as well as their purpose before permitting them access to Plaintiffs' and the Nationwide Class members' consumer credit information.

64. Equifax's failure to adopt and maintain such protective procedures directly and proximately resulted in the theft of and improper access to Plaintiffs' and the Nationwide Class members' consumer and credit information as well as its wrongful dissemination to unauthorized third parties in the public domain.

3. Violations of 15 U.S.C. §1681b(a) – Furnishing Consumer Data Without a Permissible Purpose

65. 15 U.S.C. § 1681b provides that a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id.*

66. FCRA defines a "consumer report" as: "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b)." 15 U.S.C. § 1681a(d)(1).

67. Plaintiffs' and the Nationwide Class members' personally-identifying and other

consumer information including their names, social security numbers, credit card numbers, account numbers, credit history, and other credit data constitute a "consumer report" within the meaning of 15 U.S.C. § 1681a(d)(1) because that information bears on their credit-worthiness, personal characteristics, and character and was collected by Equifax for the purpose of establishing their eligibility for credit.

68. Equifax violated § 1681b by furnishing and/or providing a written, oral, or other communications and/or documents and files which contained Plaintiffs' and the Nationwide Class members' personally-identifying and other consumer information to unauthorized third parties, who Equifax had no reason to believe would use the information for a permissible purpose.

4. Violations of 15 U.S.C. §1681b(g) – Willful Disclosure of Confidential Medical Data

69. In addition to ensuring the protection of personal consumer credit data, FCRA lays out special requirements for consumer reporting agencies with respect to confidential medical information, and restricting its dissemination or disclosure. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681 c(a)(6).

70. Upon information and belief Equifax maintains "medical information" as a component of its effort to assess the credit-worthiness of consumers. Indeed, according to a review published by the Federal Reserve, nearly half of debt collection tradelines on credit reports are for medical debts. See Robert Avery, Paul Calem, Glenn Canner, & Raphael Bostic, An Overview of Consumer Data and Credit Reporting, Fed. Reserve Bulletin (RB), p. 69 (Feb. 2003).

71. Equifax violated § 1681b by disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and the Nationwide Class members, as detailed herein, and they were harmed as a result.

5. Violations of 15 U.S.C. §1681c-1 – Willful Failure to Respond to Suspected Identify Theft

72. 15 U.S.C. §1681c-1 imposes obligations on consumer reporting agencies like Equifax upon suspicion of fraud or identity theft.

73. Specifically, §1681c-1 provides that "[u]pon the direct request of a consumer, or an individual acting on behalf of . . . of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency shall . . . include a fraud alert in the file of that consumer . . . for a period of not less

than 90 days . . . and refer the information regarding the fraud alert . . . to each of the other consumer reporting agencies," and provide certain disclosures to consumers as noted in §1681c-1(a)(2). *See* 15 U.S.C. §1681c-1(a)(2).

74. On information and belief, Equifax was given notice of that fact that millions of consumers were at risk of becoming the victim of fraud and identity theft due to the unprecedented Data Breach described above, more than one month before it was made known to the public.

75. Nevertheless, and in violation of its obligations under 15 U.S.C. §1681c-1, Equifax did not make timely disclosures to affected consumers, did not include fraud alerts to prevent identity theft following the Data Breach, and did not make timely notifications to other consumer reporting agencies; as a result, in addition to the harm described herein, Plaintiffs and the Nationwide Class were put at additional risk of fraud and identity theft, and were forced to incur additional costs to prevent the theft themselves.

6. Plaintiffs and the Nationwide Class Suffered Damages as a Proximate Result of Equifax's Willful Violations of FCRA and are Entitled to Relief

76. Equifax willfully violated the above-described provision of FCRA. The willful nature of Equifax's violations is supported by'' Equifax's other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

77. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), *1990 Commentary On The Fair Credit Reporting Act*. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

78. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

79. As a direct and proximate result of Equifax's willful violations of FCRA, and the resulting Data Breach described above, the personally-identifying and consumer credit information of Plaintiffs and the Nationwide Class members was stolen and made accessible to unauthorized third parties in the public domain.

80. As a direct and proximate result of Equifax's willful violations of FCRA, and the resulting Data Breach described above, Plaintiffs and Nationwide Class members were and continue to be damaged in the form of, without limitation, an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

81. As a result of Equifax's willful failure to "to comply with any requirement imposed under" the Act, it is liable to Plaintiffs and the Nationwide Class members for actual and statutory damages, together with their fees and costs. *See* 15 U.S.C. § 1681n (discussing willful noncompliance).

82. Plaintiffs and the Nationwide Class members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) an increased cost of credit associated with misuse of their credit data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach described above; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their personally-identifying information, personal health information, and credit data for which there is a well-established national and international market; (v) anxiety and emotional distress; together with (vi) statutory damages of not less than $100, and not more than $1000, each; and (vii) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT II —
Negligent Violation of the Fair Credit Reporting Act

83. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

84. Plaintiffs and the Nationwide Class bring this claim to recover damages suffered as a

result of Equifax's below-described negligent violations of the Fair Credit Reporting Act (herein, "FCRA" or "the Act"), 15 U.S.C. § 1681 *et seq*.

85. As detailed above, as individuals, Plaintiffs and Nationwide Class members are consumers entitled to the protections of FCRA, 15 U.S.C. § 1681a(c), and 15 U.S.C. § 1681a(f).

86. Equifax is a consumer reporting agency under FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. 15 U.S.C. § 1681 a(f).

87. As detailed above, Equifax failed to fulfill its statutory obligations under the Act by, at a minimum: (a) failing to adopt reasonable procedures to protect the confidentiality, privacy, and proper utilization of Plaintiffs and the Nationwide Class members' personal consumer, credit, and other personally-identifying information including their names, social security numbers, credit card numbers, account numbers, credit histories and other credit data; (b) furnishing and/or disclosing that information to improper third parties; (c) failing to take swift action upon learning of unauthorized access to Plaintiffs and the Nationwide Class members' personal information and its unauthorized dissemination to third parties; and (d) disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and Nationwide Class members.

88. Specifically, Equifax violated FCRA by willfully and/or negligently (1) failing to adopt and maintain reasonable procedures to protect the confidentiality of consumer information in violation of 15 U.S.C. § 1681e; (2) furnishing and/or disclosing consumer information to unauthorized third parties without a permissible purpose in violation of 15 U.S.C. § 1681b; (3) disclosing confidential medical information in violation of 15 U.S.C. §§ 1681b(g)(4), and 1681b(g)(3)(A); and (4) failing to respond to identity theft or the suspicion of identity theft in violation of 15 U.S.C. §§ 1681c-1..

89. 15 U.S.C. § 1681b provides that a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id*.

90. FCRA defines a "consumer report" as: "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b)." 15 U.S.C. § 1681a(d)(1).

91. Plaintiffs and the Nationwide Class members' personally-identifying and other consumer information including their names, social security numbers, credit card numbers, account numbers, credit history, and other credit data constitute a "consumer report" within the meaning of 15 U.S.C. § 1681a(d)(1) because that information bears on their credit-worthiness, personal characteristics, and character and was collected by Equifax for the purpose of establishing their eligibility for credit.

92. Equifax violated § 1681b by furnishing and/or providing a written, oral, or other communications and/or documents and files which contained Plaintiffs and the Nationwide Class members' personally-identifying and other consumer information to unauthorized third parties, who Equifax had no reason to believe would use the information for a permissible purpose.

93. Equifax negligently violated the above-described provision of FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by Equifax's other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

94. Equifax's negligent conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under FCRA.

95. As a direct and proximate result of Equifax's negligent violations of FCRA, and the resulting Data Breach described above, the personally-identifying and consumer credit information of Plaintiffs and the Nationwide Class members was stolen and made accessible to unauthorized third parties in the public domain.

96. As a direct and proximate result of Equifax's negligent violations of FCRA, and the resulting Data Breach described above, Plaintiffs and Nationwide Class members were and continue to be damaged in the form of, without limitation, an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

97. Plaintiffs and Nationwide Class members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) an increased cost of credit associated with misuse of their credit data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach described above; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their personally-identifying information, personal health information, and credit data for which there is a well-established national and international market; (v) anxiety and emotional distress; together with (vi) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III —
Negligence

98. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

99. Equifax owed a duty to Plaintiffs and the Nationwide Class members to exercise reasonable care in safeguarding and protecting their highly sensitive and personal information. This duty included, among other things, designing, maintaining, monitoring, testing Equifax's security systems, protocols, and practices, as well as taking other reasonable security measures to protect and adequately secure the PII of Plaintiffs and Nationwide Class members from unauthorized access.

100. Equifax owed a duty to Class members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Nationwide Class members' PII.

101. Equifax owed a duty of care to Plaintiffs and Nationwide Class members because they were foreseeable and probable victims of any inadequate security practices. It was foreseeable that if Equifax did not take reasonable security measures, the PII of Plaintiffs and members of the Nationwide

Class would be stolen. Major corporations, and particularly credit rating agencies, like Equifax face a higher threat of security breaches than smaller companies due in part to the large amounts of data they possess. Equifax knew or should have known its security systems were inadequate, particularly in light of the prior data breaches that Equifax had experienced, and yet Equifax failed to take reasonable precautions to safeguard the PII of Plaintiffs and members of the Nationwide Class.

102. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Nationwide Class members' PII.

103. Equifax had a duty to timely and accurately notify Plaintiffs and Nationwide Class members if their PII was compromised so that Plaintiffs and Nationwide Class members could act to mitigate the harm caused by the loss of opportunity to control how their PII was used.

104. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Nationwide Class members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Nationwide Class members' PII; and (d) failing to provided adequate and timely notice of the breach.

105. But for Equifax's breach of its duties, Nationwide Class members' PII would not have been accessed by unauthorized individuals.

106. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Nationwide Class members.

107. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under FCRA.

108. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiffs and Nationwide Class members suffered injury, which includes but is not limited to: (1) exposure to a heightened, imminent risk of fraud, identity theft, and financial harm; (2) the loss of the opportunity to control how their PII is used; (3) the diminution in the value and/or use of their PII; (4) the compromise, publication, and/or theft of their PII; (5) out-of-pocket costs associated with the prevention, detection,

and recovery from identity theft and/or unauthorized use of financial accounts; (6) lost opportunity costs associated with the effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft, as well as the time and effort Plaintiffs and Nationwide Class members have expended to monitor their financial accounts and credit histories to guard against identity theft; (7) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (8) unauthorized use of compromised PII to open new financial accounts; (9) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (10) the continued risk to their PII, which remain in Equifax's possession and are subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives.

109. The damages to Plaintiffs and Nationwide Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

110. Plaintiffs and the Nationwide Class are also entitled to damages and reasonable attorneys' fees and costs. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT IV —
Negligence Per Se

111. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

112. Under FCRA, 15 U.S.C. §§ 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

113. Under FCRA, 15 U.S.C. §§ 168b, a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the

information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id.*

114. Defendant failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of FCRA.

115. Under 15 U.S.C. §1681c-1, FCRA imposes obligations on consumer reporting agencies like Equifax to make timely disclosures to consumers upon suspicion of fraud or identity theft.

116. Specifically, §1681c-1 provides that "[u]pon the direct request of a consumer, or an individual acting on behalf of . . . of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency shall . . . include a fraud alert in the file of that consumer . . . for a period of not less than 90 days . . . and refer the information regarding the fraud alert . . . to each of the other consumer reporting agencies," and provide certain disclosures to consumers as noted in §1681c-1(a)(2). *See* 15 U.S.C. §1681c-1(a)(2).

117. On information and belief, Equifax was given notice of the fact that millions of consumers were at risk of becoming the victim of fraud and identity theft due to the unprecedented Data Breach described above, months before it was made known to the public.

118. Nevertheless, and in violation of its obligations under 15 U.S.C. §1681c-1, Equifax did not make timely disclosures to affected consumers, did not include fraud alerts to prevent identity theft following the Data Breach, and did not make timely notifications to other consumer reporting agencies; as a result, in addition to the harm described herein, Plaintiffs and the Nationwide Class were put at additional risk of fraud and identity theft, and were forced to incur additional costs to prevent the theft themselves.

119. Under 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681 c(a)(6), FCRA imposes requirements for consumer reporting agencies with respect to confidential medical information, and restricting its dissemination or disclosure. In violation of these obligations, Equifax disclosed, exposed, and/or made known to unauthorized third parties, the medical information of Plaintiffs and the Nationwide Class members.

120. Plaintiffs and the Nationwide Class members are within the class of persons that FCRA

was intended to protect.

121. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's violation of FCRA. Equifax knew or should have known that a breach of its data security systems would cause injuries to Nationwide Class members.

122. Equifax likewise violated Section 5(a) of the FTC Act, which provides that 'unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful." 15 U.S.C. § 45(a)(1).

123. By failing to use reasonable measures to protect consumers' PII and by not complying with applicable industry standards as discussed above, Equifax violated Section 5 of the FTC Act. Equifax's conduct was particularly unreasonable given the sensitive nature and vast amount of PII it had collected, obtained and stored, and the foreseeable consequences that a data breach of this information would substantially harm Plaintiffs and the Nationwide Class.

124. Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

125. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4

126. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

127. Further, when Equifax became aware of "unauthorized access to sensitive customer

information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.*

128. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Nationwide Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Nationwide Class members' PII.

129. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

130. Equifax also violated the GLBA by failing to notify affected consumers as soon as possible after it became aware of unauthorized access to sensitive customer information.

131. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Nationwide Class members themselves would cause damages to Nationwide Class members.

132. Defendant's failure to comply with the applicable laws and regulations, including FCRA, the FTC Act and the GLBA, constitutes negligence *per se*.

133. But for Equifax's violation of the applicable laws and regulations, Nationwide Class members' PII would not have been accessed by unauthorized individuals.

134. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and the Nationwide Class members suffered, and continue to suffer, injuries, which include but are not limited

to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Nationwide Class members must more closely monitor their financial accounts and credit histories to guard against identity theft. Nationwide Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Nationwide Class members' PII has also diminished the value of their PII.

135. Therefore, Plaintiffs and Nationwide Class members are entitled to damages in an amount to be proven at trial.

COUNT V —
Declaratory Judgment

136. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

137. As previously alleged, Plaintiffs and the Nationwide Class have stated claims against Equifax based on negligence and statutory violations.

138. Equifax has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiffs and the Nationwide Class.

139. Equifax still possesses PII pertaining to Plaintiffs and Nationwide Class members.

140. In addition, the Data Breach has rendered Equifax's system even more vulnerable to unauthorized access and requires that Equifax immediately take even more stringent measures to currently safeguard the PII of Plaintiffs and the Nationwide Class going forward.

141. Equifax has made no representation that it has remedied the vulnerabilities in its data security systems.

142. An actual controversy has arisen in the wake of the Data Breach regarding Equifax's *current* obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Nationwide Class. On information and belief, Equifax maintains that its security measures were, and remain, reasonably adequate. On information and belief, Equifax further denies that it previously had or now has any obligation to better safeguard the PII of Plaintiffs and the Nationwide Class.

143. Plaintiffs thus seek a declaration that to comply with its existing obligations, Equifax must implement specific additional, prudent industry security practices, as outlined below, to provide

reasonable protection and security to the PII of Plaintiffs and the Nationwide Class.

144. Specifically, Plaintiffs and the class seek a declaration that (a) Equifax's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, Equifax must implement and maintain reasonable security measures on behalf of Plaintiffs and the Nationwide Class, including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, data not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems Equifax uses to store the personal information of Plaintiffs and the Nationwide Class members; (8) meaningfully educating Plaintiffs and the Nationwide Class members about the threats they face as a result of the loss of their PII to unauthorized third parties, as well as the steps they must take to protect themselves; and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Nationwide Class members.

Claims Asserted on Behalf of the California Statewide Class

COUNT VI —
Violation of the California Customer Records Act
California Civil Code Section 1798.80 *et seq.*

145. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

146. Plaintiffs Kerri Murphy and Deesa Ali bring this cause of action on behalf of the California Statewide Class.

147. The California Legislature enacted Civil Code section 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain

reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

148. Equifax is a "business" as defined by Civil Code section 1798.80(a).

149. Each Plaintiff and member of the California Statewide Class is an "individual" as defined by Civil Code section 1798.80(d).

150. The information taken in the Data Breach was "personal information" as defined by Civil Code sections 1798.80(e) and 1798.81.5(d), which includes "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

151. The breach of the personal information of over 140,000 consumers was a "breach of the security system" of Equifax as defined by Civil Code section 1798.82(g).

152. By failing to implement reasonable security measures appropriate to the highly sensitive and confidential nature of consumers' personal information, Equifax violated Civil Code section 1798.81.5.

153. In addition, by failing to immediately notify all affected consumers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the Data Breach, Equifax violated Civil Code section 1798.82 of the same title. Equifax's failure to immediately notify consumers of the breach caused California Statewide Class members to suffer damages because they have lost the opportunity to immediately: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges; (v) place and renew credit fraud alerts on a

quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

154. Because it violated Civil Code sections 1798.81.5 and 1798.82, Equifax "may be enjoined" under Civil Code section 1798.84(e).

155. Plaintiffs request that the Court enter an injunction requiring Equifax to implement and maintain reasonable security procedures to protect California Statewide Class members' PII, including, but not limited to, ordering that Equifax: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, data not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems Equifax uses to store consumers' personal information; (8) meaningfully educate Plaintiffs and California Statewide Class members about the threats they face as a result of the loss of their PII to unauthorized third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and California Statewide Class members.

156. Plaintiffs further request that the Court order Equifax to (1) identify and notify all members of the class who have not yet been informed of the Data Breach; and (2) notify affected consumers of any future data breaches by email within 24 hours of Equifax's discovery of a breach or possible breach and by mail within 72 hours.

157. As a result of Equifax's violations of Civil Code sections 1798.81.5 and 1798.82,

Plaintiffs and members of the California Statewide Class have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, which remain in Equifax's possession and are subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the California Statewide Class members.

158. Plaintiffs seek all remedies available under Civil Code section 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT VII —
Violation of The Unfair Competition Law
California Business and Professions Code Section 17200 *et seq.*

159. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

160. Plaintiffs Kerri Murphy and Reesa Ali bring this cause of action on behalf of the California Statewide Class.

161. California's Unfair Competition Law ("UCL"), California Business & Professions Code § 17200, *et seq.*, provides for relief where a defendant's acts, omissions, and practices are shown to be unlawful, unfair, and fraudulent. Equifax's acts, omissions, and practices constitute unlawful and unfair

business practices in violation of the UCL.

162. Equifax's acts, omissions, and practices constitute unlawful practices and in violation of the Customer Records Act, FCRA, the FTC Act, California Civil Code §§ 1572, 1573, 1709, 1711, 1798.82, 1798.84; California Business & Professions Code §§ 17200, *et seq.*; California Business & Professions Code 17500, *et seq.*, and California common law because Equifax failed to take adequate security measures in protecting the confidentiality of Plaintiffs' and the California Statewide Class members' PII, Equifax unreasonably delayed informing Plaintiffs and the California Statewide Class about the Data Breach, and Equifax negligently released Plaintiffs' and California Statewide Class members' PII that was within its possession and control.

163. Equifax's acts, omissions, and conduct constitute unlawful practices because they failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977, the Customer Records Act, FCRA, and FTC Act which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal or medical data utilize reasonable data security measures. Equifax engaged in conduct that undermines or violates the stated policies underlying the California Customer Records Act and other privacy statutes. For instance, in enacting the Customer Records Act, the California Legislature stated that "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). Similarly, the Information Practices Act of 1977 was enacted to protect individuals' data and ensure that entities who solicit or are entrusted with personal data use reasonable security measures.

164. Equifax's acts, omissions, and conduct also constitute unfair business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiffs and California Statewide Class members. The gravity of harm resulting from Equifax's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Equifax's legitimate business interests. Equifax's conduct undermines public policy reflected in statutes such as FCRA and the FTC Act.

165. Equifax's acts, omissions, and conduct further constitute unfair business acts or practices

because Plaintiffs and California Statewide Class members have been substantially injured by the negligent release of their PII, which outweighs any countervailing benefits to Plaintiffs and California Statewide Class members.

166. Equifax engaged in fraudulent business acts or practices by representing to Plaintiffs and California Statewide Class members that they maintain adequate data security practices and procedures to safeguard PII from unauthorized disclosure, release, data breaches, and theft, and that they would comply with relevant federal and state laws pertaining to the privacy and security of PII. Had Plaintiffs and California Statewide Class members known about Equifax's substandard data security practices, they would have taken steps to protect themselves from harm that could result from Equifax's substandard data security practices.

167. Equifax engaged in fraudulent business acts or practices by omitting, suppressing, and concealing the material fact of the inadequacy of the data security protections for the PII of Plaintiffs and California Statewide Class members. Equifax failed to disclose to Plaintiffs and California Statewide Class members that Equifax's computer systems and data security practices and measures failed to meet legal and industry standards, were inadequate to safeguard their PII and that the risk of data breach or theft was highly likely. Had Plaintiffs and California Statewide Class members known about Equifax's substandard data security practices, they would have taken steps to protect themselves from harm that could result from Equifax's substandard data security practices.

168. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and California Statewide Class members. Equifax's failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer. Equifax knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and members of the California Statewide Class; and (b) defeat Plaintiffs' and the California Statewide Class members' ordinary, foreseeable and reasonable expectations concerning the security of Equifax's data systems.

169. An objective, reasonable person would have been deceived by Equifax's representations about the security and protection of data in its databases and networks.

170. As a direct and proximate result of Equifax's unlawful, unfair, and fraudulent business

practices, Plaintiffs and members of the California Statewide Class have suffered injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Equifax from their unlawful and unfair practices. Equifax's conduct caused and continues to cause substantial injury to Plaintiffs and California Statewide Class members. Equifax will continue to maintain Plaintiffs' and California Statewide Class members' PII for the indefinite future. Unless injunctive relief is granted, Plaintiffs and California Statewide Class members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and California Statewide Class members.

171. Plaintiffs and California Statewide Class members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the California Statewide Class have an effective remedy, including enjoining Equifax from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under the UCL.

172. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.X

Claims Asserted on Behalf of the Florida Statewide Class

COUNT VIII —
Violation of Florida's Unfair & Deceptive Trade Practices Act, Fla. Stat. § 501.201, et seq.

173. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

174. Plaintiff Roy Bishop brings this cause of action on behalf of the Florida Statewide Class.

175. Plaintiff and the Florida Statewide Class members are "consumers" within the meaning of Fla. Stat. § 501.203(7).

176. Equifax is engaged in "trade" or "commerce" within the meaning of Fla. Stat. § 501.203(8).

177. The Florida Unfair and Deceptive Trade Practices Act ("FUDTPA") makes unlawful "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce …" Fla. Stat. § 501.204(1).

178. In the course of their business, Equifax, through their agents, employees, and/or subsidiaries, violated the FUDTPA as detailed above. Specifically, by failing to take reasonable

measures to protect consumer identifying information, failing to promptly notify consumers of the breach of that information, and failing to otherwise adequately prepare for or respond to the breach, Equifax engaged in one or more of the following unfair or deceptive acts or practices prohibited by Fla. Stat. § 501.204(1):

- Failing to maintain adequate and reasonable data security standards to safeguard Florida Statewide Class members' sensitive information from unauthorized disclosure, release, data breaches, and theft, in violation of state and federal laws and its own privacy practices and policies;
- Knowingly and fraudulently misrepresenting that it would maintain adequate and reasonable data security standards for Florida Statewide Class members' sensitive information and safeguard Florida Subclass members' sensitive information from unauthorized disclosure, release, data breaches, and theft;
- Knowingly omitting, suppressing, and concealing the inadequacy of its data security protections for the Florida Statewide Class members' sensitive information;
- Failing to disclose the Data Breach to the Florida Statewide Class members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4); and

179. Defendant's concealment of its data security shortcomings was material to Plaintiff and the Florida Statewide Class, as Defendant intended. Had they known the truth, Plaintiff and the Florida Statewide Class would have taken steps to prevent Equifax from obtaining their personal identifying information.

180. Plaintiff and Florida Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not make public that information. Plaintiff and Florida Statewide Class members did not, and could not, unravel Defendant's deception on their own.

181. Defendant had an ongoing duty to Plaintiff and the Florida Statewide Class to refrain from unfair and deceptive practices under the FUDTPA in the course of its business. Specifically, Defendant owed Plaintiff and Florida Statewide Class members a duty to disclose all the material facts concerning the measures taken to protect class members' sensitive information because they possessed exclusive knowledge, they intentionally concealed it from Plaintiff and the Florida Statewide Class,

and/or they made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

182. Plaintiff and Florida Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

183. Defendant's violations present a continuing risk to Plaintiff and the Florida Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

184. Pursuant to Fla. Stat. §§ 501.2105(1)-(2), Plaintiff and the Florida Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages and any other just and proper relief available under the FUDTPA.

Claims Asserted on Behalf of the Pennsylvania Statewide Class

COUNT IX —
Violation of the Pennsylvania Unfair Trade Practices And Consumer Protection Law, 73 Pa. Stat. Ann. § 201-1, et seq.

185. Plaintiff incorporate by reference all paragraphs above as if fully set forth herein.

186. Plaintiff Bruce Mattock brings this cause of action on behalf of the Pennsylvania Statewide Class.

187. Equifax and the Pennsylvania Statewide Class members are "persons" within the meaning of 73 Pa. Stat. Ann. § 201-2.(2).

188. Equifax is engaged in "trade" or "commerce" within the meaning of 73 Pa. Stat. Ann. § 201-2(3).

189. The Pennsylvania Unfair Trade Practices Act ("Pennsylvania UTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce …." 73 Pa. Stat. Ann. § 201 3.

190. In the course of its business, Equifax, through its agents, employees, and/or subsidiaries, violated the Pennsylvania UTPA as detailed above. Specifically, Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Pennsylvania Statewide Class in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the

following:

- Causing likelihood of confusion or of misunderstanding as to the security of consumer identifying information;
- Failing enact adequate privacy and security measures to protect the Pennsylvania Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Pennsylvania Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Pennsylvania Statewide Class members' PII;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or
- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and sale of credit furnishing goods and services, whether or not any person has in fact been misled, deceived or damaged thereby.

191. Defendant's concealment of its data security shortcomings was material to Plaintiff and the Pennsylvania Statewide Class, as Defendant intended. Had they known the truth, Plaintiff and the Pennsylvania Statewide Class would have taken steps to prevent Equifax from obtaining their personal identifying information.

192. Plaintiff and Pennsylvania Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not make public that information. Plaintiff and Pennsylvania Statewide Class members did not, and could not, unravel Defendant's deception on their own.

193. Defendant had an ongoing duty to Plaintiff and the Pennsylvania Statewide Class to refrain from unfair and deceptive practices under the FUDTPA in the course of their business. Specifically, Defendant owed Plaintiff and Pennsylvania Statewide Class members a duty to disclose all the material facts concerning the measures taken to protect class members' sensitive information because they possessed exclusive knowledge, they intentionally concealed it from Plaintiff and the Pennsylvania Statewide Class, and/or they made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

194. Plaintiff and Pennsylvania Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

195. Defendant's violations present a continuing risk to Plaintiff and the Pennsylvania Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

196. Pursuant to 73 Pa. Stat. Ann. § 201-9.2(a), Plaintiff and the Pennsylvania Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, punitive and/or treble damages, and any other just and proper relief available under the Pennsylvania UTPA.

Claims Asserted on Behalf of the Connecticut Statewide Class

COUNT X —
Violation of Connecticut Unlawful Trade Practices Act,
Conn. Gen. Stat. § 42-110a, *et seq.*

197. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

198. Plaintiff Nancy Gauger brings this action on behalf of himself and the Connecticut Statewide Class against Defendant.

199. Equifax and the Connecticut Statewide Class members are "persons" within the meaning of Conn. Gen. Stat. § 42-110a(3) of the Connecticut Unfair Trade Practices Act ("Connecticut UTPA"). Equifax is engaged in "trade" or "commerce" within the meaning of Conn. Gen. Stat. § 42-110a(4).

200. The Connecticut UTPA provides: "No person shall engage in unfair methods of

competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

201. In the course of its business, Defendant Equifax, through its agents, employees, and/or subsidiaries, violated the Connecticut UTPA as detailed above. Specifically, failing to adequately protect the sensitive information of Connecticut Statewide Class members and failing to adequately respond to a data breach, Defendant engaged in one or more of the following unfair or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b(a):

- Causing likelihood of confusion or of misunderstanding as to security of Connecticut Statewide Class members sensitive information;
- Representing that the Equifax's information security systems and practices have characteristics or benefits that they do not have;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or
- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and sale of Equifax's goods or services, whether or not any person has in fact been misled, deceived or damaged thereby.

202. Defendant's scheme and concealment of the true characteristics of its information security systems were material to Plaintiff and the Connecticut Statewide Class, as Defendant intended. Had they known the truth, Plaintiff and the Connecticut Statewide Class would not have permitted Equifax to retain their sensitive information.

203. Plaintiff and Connecticut Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not disclose the true nature of its information security systems and practices.

204. Defendant had an ongoing duty to Plaintiff and the Connecticut Statewide Class to refrain from unfair and deceptive practices under the Connecticut UTPA in the course of its business. Specifically, Defendant owed Plaintiff and Connecticut Statewide Class members a duty to disclose all

the material facts concerning its information security systems and practices because it possessed exclusive knowledge, they intentionally concealed it from Plaintiff and the Connecticut Statewide Class, and/or they made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

205. Plaintiff and Connecticut Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

206. Defendant's violations present a continuing risk to Plaintiff and the Connecticut Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

207. Pursuant to Conn. Gen. Stat. § 42-110g, Plaintiff and the Connecticut Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, punitive damages, and any other just and proper relief available under the Connecticut UTPA.

Claims Asserted on Behalf of the Arizona Statewide Class

COUNT XI —
Violation of Arizona Consumer Fraud Act, Ariz. Rev. Stat. Ann. §§ 44-1521, *et seq.*

208. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

209. Plaintiff Tom W. Hannon brings this action on behalf of himself and the Arizona Statewide Class against Defendant.

210. The Arizona Consumer Fraud Act prohibits "any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged."

211. Plaintiff and members of the Arizona Statewide Class are "persons" as defined by Ariz. Rev. Stat. § 44-1521(6).

212. Pursuant to Ariz. Rev. Stat. §§ 44-1521(5) and (7), Defendant engaged in the sale of "merchandise" including credit reports and identity protection.

213. Defendant engaged in deceptive acts or practices by representing to Plaintiff and the Arizona Statewide Class that they maintain data security practices and procedures to safeguard Arizona Statewide Class members' sensitive information from unauthorized disclosure, release, data breaches, and theft, and that they would comply with relevant federal and state laws pertaining to the privacy and security of sensitive information. Plaintiff and the Arizona Statewide Class members were misled by Defendant's misrepresentations and reasonably relied upon them to their detriment. Had Plaintiff and the Arizona Statewide Class members known about Defendant's substandard data security practices, they would have taken steps to protect themselves from harm that could result from Defendant's substandard data security practices.

214. Defendant engaged in deceptive acts or practices by omitting, suppressing, and concealing the material fact of the inadequacy of their data security protections for the sensitive information of Plaintiff and the Arizona Statewide Class. Defendant failed to disclose to Plaintiff and the Arizona Statewide Class that Defendant's data security systems failed to meet legal and industry standards to protect their sensitive information. Had Plaintiff and the Arizona Statewide Class members known about Defendant's substandard data security practices, they would have taken steps to protect themselves from harm that could result from Defendant's substandard data security practices.

215. Equifax knew, or should have known, that its computer systems and data security practices and measures failed to meet legal and industry standards to protect the sensitive information of Plaintiff and the Arizona Statewide Class, were inadequate to safeguard the sensitive information of Plaintiff and the Arizona Statewide Class, and that the risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Arizona Statewide Class members. Defendant's failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer. Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and members of the Arizona Statewide Class; and (b) defeat Plaintiff's and the Arizona Statewide Class members' ordinary, foreseeable and reasonable expectations concerning the adequacy of Defendant's data security.

216. An objective, reasonable person would have been deceived by Equifax's representations

about the security and protection of data in its databases and networks.

217. Defendant intended that Plaintiff and the Arizona Statewide Class rely on their deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Equifax's offering of credit reporting and identity protection services and incorporating Plaintiff's and the Arizona Statewide Class members' sensitive information on its computer systems, in violation of the Arizona Consumer Fraud Act.

218. Defendant also engaged in unfair acts and practices by failing to maintain the data security of Plaintiffs' and the Arizona Statewide Class members' sensitive information in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach.

219. Defendant's wrongful practices, which occurred in the course of trade or commerce, were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to Plaintiff and the Arizona Statewide Class and were repeated continuously before and after Defendant obtained confidential sensitive information concerning Plaintiff and Arizona Statewide Class members, all of whom have been adversely affected by Defendant conduct and the public was and is at risk as a result thereof.

220. Equifax's acts, omissions, and practices proximately caused Plaintiff and Arizona Statewide Class members to suffer damages including incurring costs associated with protecting sensitive information that has been exposed; costs associated with the theft of their identities, such as time and expenses associated with credit monitoring, decrease in credit ratings, financial harm suffered as a result of accounts opened and used without their knowledge or authorization, and time and expense associated with closing accounts opened and used without their knowledge or authorization.

221. As a direct and proximate result of Defendant's unfair and deceptive practices, Plaintiff and members of the Arizona Statewide Class have suffered injuries to legally protected interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their sensitive information, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of value of their sensitive information.

222. As a direct and proximate cause of these practices, Plaintiff and Arizona Statewide Class members suffered an ascertainable loss.

223. The above unfair and deceptive trade practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Arizona Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

224. As a direct and proximate result of Equifax's unlawful, unfair, and fraudulent business practices, Plaintiff and members of the Arizona Statewide Class have suffered injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Equifax from their unlawful and unfair practices. Equifax's conduct caused and continues to cause substantial injury to Plaintiff and Arizona Statewide Class members. Equifax will continue to maintain Plaintiff's and Arizona Statewide Class members' sensitive information for the indefinite future. Unless injunctive relief is granted, Plaintiff and Arizona Statewide Class members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Arizona Statewide Class members.

225. Plaintiff and Arizona Statewide Class members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Arizona Statewide Class have an effective remedy, including enjoining Equifax from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under Ariz. Rev. Stat. § 44-1521.

226. Plaintiff and the Arizona Statewide Class also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and the Arizona private attorney general doctrine.

Claims Asserted on Behalf of the South Carolina Statewide Class

COUNT XII —
Violation of South Carolina Data Breach Security Act, S.C. Code Ann. § 39-1-90, *et seq.*

227. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

228. Plaintiffs Ashley Cashon and Jade Haileselassie bring this action on behalf of the South

Carolina Statewide Class against Defendant.

229. Equifax is required to accurately notify Plaintiffs and South Carolina Statewide Class members following discovery or notification of a breach of its data security system (if personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm) in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

230. Equifax is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

231. Plaintiffs and South Carolina Statewide Class members' Personal Information (e.g., Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

232. Because Equifax discovered a breach of its data security system (in which personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A), but failed to do so.

233. As a direct and proximate result of Equifax's violations of S.C. Code Ann. § 39-1-90(A), Plaintiffs and South Carolina Statewide Class members suffered damages, as described above.

234. Plaintiffs and South Carolina Statewide Class members seek relief under S.C. Code Ann. § 39-1-90(G), including, but not limited to, actual damages and injunctive relief.

COUNT XIII —
Violations of South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-10, *et seq.*

235. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

236. Plaintiffs Ashley Cashon and Jade Haileselassie bring this action on behalf of the South Carolina Statewide Class against Defendant.

237. Equifax, Plaintiffs, and the South Carolina Statewide Class members are "persons" within the meaning of S.C. Code § 39-5-10(a).

238. Equifax is engaged in "trade" or "commerce" within the meaning of S.C. Code § 39-5-

10(b).

239. The South Carolina Unfair Trade Practices Act ("South Carolina UTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code § 39-5-20(a).

240. In the course of its business, Equifax, through its agents, employees, and/or subsidiaries, violated the South Carolina UTPA as detailed above. Specifically, in failing to adequately protect the sensitive information of South Carolina Statewide Class members and failing to adequately respond to a data breach, Defendant engaged in one or more of the following unfair or deceptive acts or practices in violation of S.C. Code § 39-5-20(a):

- Causing likelihood of confusion or of misunderstanding as to security of South Carolina Statewide Class members sensitive information;
- Representing that the Equifax's information security systems and practices have characteristics or benefits that they do not have;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or
- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and sale of Equifax's goods or services, whether or not any person has in fact been misled, deceived or damaged thereby.

241. Defendant's scheme and concealment of the true characteristics of its information security systems were material to Plaintiffs and the South Carolina Statewide Class, as Defendant intended. Had they known the truth, Plaintiffs and the South Carolina Statewide Class would not have permitted Equifax to retain their sensitive information.

242. Plaintiffs and South Carolina Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not disclose the true nature of its information security systems and practices.

243. Defendant had an ongoing duty to Plaintiffs and the South Carolina Statewide Class to refrain from unfair and deceptive practices under the South Carolina UTPA in the course of its business.

Specifically, Defendant owed Plaintiffs and South Carolina Statewide Class members a duty to disclose all the material facts concerning its information security systems and practices because it possessed exclusive knowledge, they intentionally concealed it from Plaintiffs and the South Carolina Statewide Class, and/or they made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

244. Plaintiffs and South Carolina Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

245. Defendant's violations present a continuing risk to Plaintiffs and the South Carolina Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

246. Pursuant to S.C. Code § 39-5-140(a), Plaintiffs and the South Carolina Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, treble and/or punitive damages, and any other just and proper relief available under the South Carolina UTPA.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Nationwide Class and Statewide Classes, respectfully request:

247. An order certifying the proposed Class or Classes under the provisions of Rule 23 of the Federal Rules of Civil Procedure, and directing that notice be provided to all members of the Classes;

248. A finding that Equifax breached its duty to safeguard and protect the PII of Plaintiffs and Nationwide Class members that was compromised in the Data Breach;

249. Injunctive relief, including public injunctive relief in the form of an order enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

250. That Plaintiffs and Nationwide Class members recover damages in the form of restitution or disgorgement and/or compensatory damages for economic loss and out-of-pocket costs, treble damages under the applicable federal and state laws, and punitive and exemplary damages under

applicable law;

251. A determination that Equifax is financially responsible for all Class notice and administration of Class relief;

252. A judgment against Defendant for any and all applicable statutory and civil penalties;

253. An order requiring Defendant to pay both pre- and post-judgment interest on any amounts awarded;

254. An award to Plaintiffs and Nationwide Class members of costs and reasonable attorneys' fees;

255. Leave to amend this Complaint to conform to the evidence produced in discovery and at trial; and

256. Such other or further relief as the Court may deem appropriate, just, and equitable.

IX. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable.

DATED this 11th day of September, 2017.

KELLER ROHRBACK L.L.P.

By _____

Matthew J. Preusch (298144)
mpreusch@kellerrohrback.com
801 Garden Street, Suite 301
Santa Barbara, CA 93101
(805) 456-1496, Fax (805) 456-1497

Lynn Lincoln Sarko, *pro hac vice forthcoming*
Derek W. Loeser, *pro hac vice forthcoming*
Gretchen Freeman Cappio, *pro hac vice forthcoming*
Cari Campen Laufenberg, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900, Fax (206) 623-3384
lsarko@kellerrohrback.com
dloeser@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com

MOTLEY RICE LLC

Jodi Flowers, *pro hac vice forthcoming*
Breanne Cope (260217)
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
(843) 216-9000, Fax (843) 216-9450
jflowers@motleyrice.com
bcope@motleyrice.com

Laura Ray, *pro hac vice forthcoming*
Mathew Jasinski, *pro hac vice forthcoming*
One Corporate Center
20 Church Street
17th Floor
Hartford, CT 06103
(860) 882-1681, Fax (860) 882-1682
lray@motleyrice.com
mjasinski@motleyrice.com

Attorneys for Plaintiffs